УДК 621.371.3

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОЛУЧЕННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТЕОРНОГО РАДИОКАНАЛА

И.Е. Антипов
Доктор технических наук, профессор, заведующий кафедрой*
E-mail: i_ant@mail.ru

М.А. Шернин
Аспирант*
E-mail gxaski@mail.ru
*Кафедра основ радиотехники
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166
Контактный тел.: (057) 700-22-84

Розглянуті статистичні характеристики випадкових числових послідовностей, отриманих на підставі експериментальних даних шляхом обчислення інтервалів між метеорними слідами і пропозиції по їх поліпшенню

Ключові слова: метеорний радіоканал, випадкова числова послідовність

Рассмотрены статистические характеристики случайных числовых последовательностей, полученных на основании экспериментальных данных путём вычисления интервалов между метеорными следами и предложения по их улучшению

Ключевые слова: метеорный радиоканал, случайная числовая последовательность

Statistical descriptions of casual numerical sequences, got on the basis of experimental information by the calculation of intervals between meteor tracks and suggestion on their improvement

Keywords: meteor radio channel, casual numerical sequence

1. Введение

В работах [1] показано, что интервалы между метеорными следами являются случайными и известными обоим корреспондентам, связанным между собой по данному метеорному радиоканалу. Измерение этих интервалов позволяет формировать числовые случайные последовательности (ЧСП), одинаковые в обоих пунктах.

Остаётся открытым вопрос о законе распределения этих случайных величин и о возможной взаимосвязи между отдельными случайными значениями. В статье анализируются экспериментальные данные, которые позволяют найти ответы на эти вопросы. Также предлагаются пути улучшения статистических характеристик ЧСП.

2. Преобразование закона распределения случайных значений

В зависимости от мощности передатчиков, длины трассы и времени суток время между метеорными следами может составлять от нескольких секунд до десятков минут. На рис. 1 ступенчатой линией показан экспериментально полученный закон распределения времени ожидания для системы синхронизации по МРК [2].

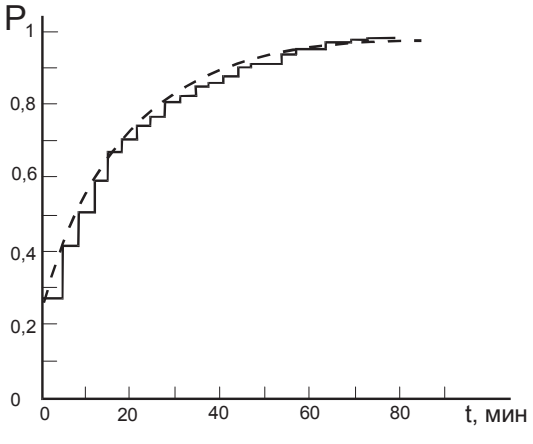

Рис. 1. Время ожидания сеанса метеорной связи

Представленную зависимость можно аппроксимировать выражением:

$$F(t) = 1 - \exp\left(\frac{-t-6}{20}\right), \quad (1)$$

график которого представлен на рис. 1 пунктирной кривой.

Как видно, закон распределения не является равномерным. Для повышения криптографической стойкости метода, его следует преобразовать в равномерный.

Для непрерывной случайной величины задача ставится следующим образом: зная плотность распределения случайной величины X и плотность распределения случайной величины $Y=\varphi(X)$, необходимо найти функцию отображения $\varphi(X)$.

Пусть $f_x(x)$ - плотность распределения случайной величины X и $f_y(y)$ - плотность распределения вероятности случайной величины Y. Обозначим через $y=\varphi(x)$ - некоторую монотонную и дифференцируемую функцию. Тогда:

$$f_y(y)=f_x(x)\frac{dx}{dy}=f_x(\varphi^{-1}(y))\frac{d}{dy}(\varphi^{-1}(y)), \quad (2)$$

где $\varphi^{-1}(y)$ - обратная функция к функции $y=\phi(x)$, то есть $x=\varphi^{-1}(y)$.

Найдём плотность вероятности ожидания сеанса связи:

$$f(t)=\frac{dF(t)}{dt}=\frac{1}{20}e^{\frac{-t-6}{20}}. \quad (3)$$

Пусть максимальное время ожидания метеорного следа составит 30 минут, тогда необходимая плотность вероятности имеет следующий вид:

$$f(z)=\begin{cases}\frac{1}{30}, & z\in(0,30),\\ 0, & z\notin(0,30).\end{cases} \quad (4)$$

Будем искать требуемую зависимость между величинами Z и t в виде монотонной возрастающей функции $z=\varphi(t)$, для которой по условию

$$f_z(z)=f_t(\varphi^{-1}(z))\frac{d}{dz}(\varphi^{-1}(z)). \quad (5)$$

Получаем дифференциальное уравнение

$$\frac{1}{30}=\frac{1}{20}e^{\frac{-6}{20}}\cdot e^{\frac{-\varphi^{-1}(z)}{20}}\frac{d}{dz}(\varphi^{-1}(z)). \quad (6)$$

Решение этого уравнения при начальном условии $\varphi(0)=0$ будет иметь вид

$$Z=30\cdot e^{-\frac{3}{10}}\cdot(1-e^{-\frac{t}{20}}),t\in(0,30). \quad (7)$$

Таким образом, подвергнув случайную величину t с экспоненциальным законом распределения функциональному преобразованию (7), можно получить случайную величину Z, равномерно распределенную на интервале (0, 30).

3. Статистическое тестирование

Перед использованием сформированной ЧСП в качестве криптографического ключа, необходимо убедиться в том, что она действительно случайна. Наличие закономерностей в ключе приводит к неявному уменьшению его размера и, следовательно, к понижению криптографической стойкости.

Для проверки вероятностных характеристик ЧСП были использованы данные, полученные на радиометеорном комплексе МАРС в августе 2006 г. (Мощность передатчика 400 кВт, несущая частота 31,5 МГц, ДН ориентированы на восток, частота повторения импульсов 100 Гц [2]).

Наиболее известными наборами статистических тестов является набор тестов, предложенный Кнутом [3]. Согласно методике каждая битовая строка длиной 20000 битов проверяется по каждому из четырех тестов. Если какой-нибудь из тестов не выполнен, то констатируется факт, что последовательность не прошла тест. Решение о прохождении теста принимается на основе проверки попадания вычисляемых значений статистических параметров в доверительную область, рассчитанную для заданного уровня значимости. Используются следующие четыре теста.

1) Монобитный тест. Это самый простой тест. Он основан на равенстве частот 1 и 0 в идеальной ЧСП. Если X и Y обозначить как количество нулей и единиц в последовательности из 20 000 бит (b), то

$$X=\sum_{j=1}^{20000}b_j. \quad (8)$$

Если последовательность случайная, то значения X должно лежать в интервале $9\,725 < X < 10\,275$. Единственной сложностью здесь является эффективный подсчет числа различных битов, т. к. в большинстве современных вычислительных архитектур нет команд для работы с отдельными битами.

2) Покерный тест. Здесь вся проверяемая ЧСП разбивается на 5000 блоков длиной 4 бит. Этот тест, как и предыдущий, основан на том, что в идеальной ЧСП вероятность всех блоков одинакова. Пусть f(i) есть число всех 4-битных блоков, двоичное представление которых есть число i. В покерном тесте считается следующая статистическая функция:

$$X=\left(\frac{16}{5000}\right)*\left(\sum_{i=0}^{15}\left[f(i)\right]^2\right)-5000. \quad (9)$$

Тест считается пройденным, если $2.16 < X < 46.17$.

3) Серийный тест. Тест определяет число вхождений серий одинаковых битов различной длины. В идеальной ЧСП длинной L среднее число серий длиной i равняется

$$l_i=\frac{(L-i+3)}{2^{i+2}}. \quad (10)$$

Пусть $n = \max i\ (i : l_i \geq 5)$, число единичных и нулевых серий в проверяемой последовательности длиной i равняется B_i и G_i соответственно. Для последовательности длинной 20 000 имеем n = 9. Вычисляемая в тесте статистика:

$$X=\sum_{i=1}^{n}\frac{(B_i-l_i)^2}{l_i}+\sum_{i=1}^{n}\frac{(G_i-l_i)^2}{l_i} \quad (11)$$

Результат теста может вычисляться двумя способами: можно вычислять статистику X и сравнивать ее с одним порогом, либо, как реализовано в стандарте

FIPS 140-1, сравнивать с различными порогами каждое из чисел B_i и G_i. Алгоритм вычисления длины битовых блоков основан на том, что число $2^n - 1$ содержит n единичных битов. Для произвольного числа x, содержащего серию нулевых битов длиной n в младших разрядах, XOR(x, x–1) содержит серию из n+1 единичных битов в младших разрядах (все остальные биты нулевые). Длину выделенной таким образом канонической серии единичных битов можно считать бинарным поиском, либо с помощью заранее вычисленной таблицы. Если последовательность случайная, то количество серий каждой длины должно находится в интервалах, приведенных в табл. 1.

Таблица 1

Допустимые значения для теста серий

Длина серии	1	2	3	4	≥5
Допустимые значения	2310...2680	1110...1390	527...723	240...384	103...209

4) Тест длины серии. Суть теста состоит в проверке максимальной длины серии из одинаковых элементов. Если последовательность случайна, то максимальная длина серии не должна превышать значение 26, поскольку вероятность появления серии такой длины очень мала.

Анализ ЧСП, полученной в результате обработки результатов эксперимента показал, что она не прошла тест, то есть, в ней присутствуют явные закономерности. Углублённый анализ причин показал, что частота появление 0 и 1 неодинакова из-за большого количества незначащих нулей перед «короткими» числовыми значениями.

Для улучшения качества ЧСП её необходимо модифицировать. В качестве варианта модификации было предложено удалять нули, количество которых кратно 4. Модифицированная таким образом ЧСП была подвергнута повторному тесту, результаты, которого приведенные в табл. 2.

Таблица 2

Результаты тестирования

Название теста	Статистика			Результат
Монобитный тест	9681 бит			+
Покер тест	57,04			+
Серийный тест	длина	«0»	«1»	
	1	2355	2585	+
	2	1214	1246	+
	3	694	611	+
	4	500	295	+
	5	119	131	+
	≥6	121	135	+
Тест длины серии	13 бит			+

4. Выводы

Как видно, последовательность прошла предложенный тест, иначе говоря, явных закономерностей в полученной ЧСП не обнаружено. Следует также отметить, что полученные значения, находятся вблизи порога прохождения теста. Улучшения качества ЧСП возможно такими же методами, которые используются для улучшения качества выходных данных в любых генераторов случайных чисел.

Кроме того, следует обратить внимание на тот факт, что сами данные не были предназначены для оценки случайности данного метода. При получении экспериментальных данных использовался передатчик, мощность которого значительно выше мощности, которая необходима для реализации системы защиты информации с использованием МРК. Это привело к тому, что осуществлялась регистрация таких метеорных следов, доля отраженной мощности от которых, не позволила бы зарегистрировать их системой защиты на основе МРК.

Литература

1. Антипов И. Е., Костыря А. А., Шернин М.А. Использование метеорного радиоканала для формирования случайной числовой последовательности. Харьков. Коллегиум. – 2009 // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2009. Вып. 157. С. 25 - 29.
2. Антипов И. Є., Коваль Ю. А., Обельченко В. В. Развитие теории и совершенствование радиометеорных систем связи и синхронизации. - Харьков, Коллегиум, 2006, 308 с.
3. Кнут Д. Э. Случайные числа // Искусство - 3-е изд. - М.: Вильямс, 2000, 832 с.